Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017
Date filed: February 27, 2018

Name of company covered by this certification:	MegaPath Group, Inc.
Form 499 Filer ID:	822052 consolidated
Name of signatory:	Birch Blair
Title of signatory:	Vice President – Asst. General Counsel

I, Birch Blair, certify that I am an officer of MegaPath Group, Inc., and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.

The Company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The Company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The Company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____

Birch Blair
Vice President, General Counsel & Secretary
MegaPath Group, Inc.

Executed February 26, 2018

Summary Statement of CPNI Policies

MegaPath Group, Inc. and its affiliate, MegaPath Cloud Company LLC, (collectively, the "Company") has established practices and procedures to ensure its compliance with Section 222 of the Communications Act and the Commission's Customer Proprietary Network Information ("CPNI") rules set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*

The Company has procedures in place to ensure that the use, disclosure, or access to CPNI by the Company's employees, affiliates, agents, or other third parties is in accordance with the Commission's rules. The following is a summary of Company's policies and procedures related to protection of customer information:

Use and Disclosure of CPNI: The Company will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect its rights or property, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Access Limitation: The Company limits access to CPNI by employees or other entities. Employees are held to non-disclosure obligations and are subject to disciplinary action.

Training Programs: The Company conducts training to ensure that employees, affiliates, agents, and other third parties with access to CPNI adequately protect such information in accordance with the Commission's rules.

Marketing: The Company does use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to customers. Although its current policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process

Tracking Customers: The Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

Carrier Proprietary Information: When the Company receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

Avoidance of Pretexting: The Company has in place security verification procedures to ensure that changes to service may only be made by and customer account information is only provided to bona fide customers.

Call Detail Information: The Company will not disclose Call Detail Information to an inbound caller, unless the customer provides a password or back-up authentication that does not prompt

the customer for readily available biographical or account information. Customers seeking Call Detail Information may request that it be sent to their address of record or the Company may provide it by calling the customer's telephone number of record.

Online Access to CPNI: To access an on-line account from which a customer can access their CPNI, the customer must enter their login ID and CPNI Password.

In-Person Access to CPNI: Company does not routinely make CPNI available at its offices. However, in the event that a customer requests CPNI in person, Company may disclose a customer's CPNI to an authorized person only upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

Notice of Account Changes: The Company will send a notice to customer's pre-existing address of record notifying them of a change whenever a password, online account, or address of record is changed. The notices will not reveal the changed information.

Notification of CPNI Breaches: In accordance with the Commission's rules, the Company has in place a system to notify the federal government and customers of breaches that occur when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

Record Retention: Company will maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the US Secret Service and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Company maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Company later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission's recordkeeping requirements. Company maintains a record of all customer complaints related to their handling of CPNI, and records of Company's handling of such complaints, for at least two years.